```
     (FILE 'USPAT' ENTERED AT 08:41:15 ON 15 JUL 1999)
L1            12 S IDENTIF? (P) PROJECTOR# (P) COMPUTER (P) CONNECT###
L2             0 S 5887147/UREF
L3             1 S 5887147/PN
L4          2853 S INFORMATION (P) (DISPLAY OR SCREEN) (P) MATCH###
L5           130 S L4/AB
L6            30 S EXTERNAL### (P) COMPUTER# (P) L4
L7           118 S (IDENTIF? (3W) INFORMATION) (P) (DISPLAY OR SCREEN) (P)
MAT
L8             8 S L7/AB
L9            17 S COLOR# (P) SIZE# (P) (DISPLAY OR SCREEN) (P) (IDENTIF? (
3W)
L10          207 S MATCH### (P) (PERMISSION OR ACCESS###) (P) (INFORMATION
OR
L11           20 S (DISPLAY OR SCREEN) (P) L10
L12          138 S COMPAR### (P) MATCH### (P) (ID OR PASSWORD#) (P) (DISPLA
Y O
L13            0 S L12/AB
L14           27 S COMPUTER (P) L12
L15            6 S PASSWORD# (P) CARD# (P) COMPUTER (P) PERMISSION#
L16          163 S (SECUR? (3A) CARD#) (P) (PERMI##### OR ALLOW###) (P) ACC
ESS
L17           32 S COMPUTER# (P) L16
L18          234 S SECURITY (P) (DISPLAY (2W) (DEVICE# OR APPARATUS))
L19            2 S (ID OR PASSWORD#) (P) MATCH### (P) L18
L20            7 S (ID OR IDENTIF?) (P) MATCH### (P) L18
L21          172 S (ID OR IDENTIF?) (P) MATCH### (P) (DISPLAY### (3W) (DEVI
CE#
L22           13 S L21/AB
L23           15 S COMPAR### (P) L21 (P) COMPUTER#
```

US PAT NO: 5,599,231 [IMAGE AVAILABLE] L23: 5 of 15
TITLE: Security systems and methods for a videographics and authentication game/program fabricating device

CLAIMS:

CLMS(4)

4. A method for restricting the play and copying of video games to authorized users of an interactive **computer** system having a **display** screen, an **identification device** interface, a removable disk drive and a game cartridge interface, comprising the following steps:

a. reading an **identification** code stored on an **identification** device inserted into the **identification** device interface;

b. **comparing** the **identification** code read from the **identification** device to an **identification** code read from a related game program file stored on a removable disk inserted in the removable disk drive;

c. enabling the **computer** system to copy the game program file, if a predetermined relationship exists between the **identification** codes read from the **identification** device and from the related game program filed stored on the removable disk;

d. editing the game program file to create. . . program stored on the game cartridge; and

g. inhibiting the editing of the game program file in step (d) if the **identification** codes do not **match** in step (c) while permitting game play if the game cartridge is authenticated in step (e).

CLAIMS:

CLMS(13)

13. A method for restricting the displaying and copying of video games to authorized users of a **computer** system having a **display** screen, an **identification device** interface, a memory drive device and a read only videographics program storage interface, comprising the following steps:

a. reading an **identification** code stored on an **identification** device inserted into the **identification** device interface;

b. **comparing** the **identification** code read from the **identification** device to an **identification** code read from a related videographics program file stored on a memory unit inserted in the memory drive device;

c. if a predetermined relationship exists between the **identification** codes stored in the **identification** device and memory unit, enabling the **computer** system to copy the videographics program file, and

d. editing the videographics program file to create a videographics program derived from. . . videographics to the videographics storage device,

f. displaying the videographics, and

g. inhibiting the editing of videographics in step (d) if the **identification** codes do not **match** in step (c) while permitting the display of videographics if the videographics storage device is authenticated in step (e).

=> d ti kwic 11

US PAT NO: 5,623,637 [IMAGE AVAILABLE] L17: 11 of 32
TITLE: Encrypted data storage card including smartcard integrated circuit for storing an access password and encryption keys

SUMMARY:

BSUM(15)

In . . . the form of a "smartcard" integrated circuit capable of storing secret key values which may be used to provide password-protected **access** to the data stored on the memory card, or optionally to provide secure storage for the encryption or decryption keys, or digital signatures, needed to **allow** the host **computer** to **access** and/or operate a secure information storage or telecommunications system. In accordance with the invention, **access** to data, passwords, digital signatures, or other key values stored on the memory card is limited to those who (1) have physical possession of the memory card and (2) knowledge of the memory card **access** password stored in the **card**'s **secure** substorage unit.

US PAT NO: 5,191,611 [IMAGE AVAILABLE] L14: 19 of 27
TITLE: Method and apparatus for protecting material on storage media and for transferring material on storage media to various recipients

SUMMARY:

BSUM(9)

For . . . would correctly enter his particular personal identification code in the aforementioned smart card PAD to activate it, which would then **display** both the ZAC as well as the system identification code in either encrypted or non-encrypted form. The user, utilizing a keyboard, would enter this code into the **computer** which then **compares** the decrypted or encrypted codes obtained from both the smart card and CD ROM and if a **match** is obtained, would then verify that this particular system identification (**ID**) code is proper and that material this accessor seeks access to is stored on the storage medium or media. The **computer** then retrieves the paired personal security key (SK). The **computer** would then generate a random number which is displayed upon its **screen** to serve as a challenge to the personal accessing device (smart card). The user would input this random number into the smart card via its keypad. The smart card as well as the **computer** are provided with a particular encryption/decryption algorithm (alternately a security processor chip). Both the **computer** and the smart card would simultaneously compute a response to the challenge code (random number) and this response is displayed on the smart card's **display screen**. This displayed response is then entered into the **computer** through its keyboard to determine whether there is a **match**. If a **match** is shown to have occurred, the **computer** will then **display** all the material names (directories) therein for the logical zones which access privileges have been granted and allow the user. . .

US PAT NO: 4,754,326 [IMAGE AVAILABLE] L14: 25 of 27
TITLE: Method and apparatus for assisting user of information retrieval systems

DETDESC:

DETD(212)

Normally, the user positions the cursor successively in each box depicted on the video **screen**, types in the same **password** in each place, and then touches the Action key. The two entries are then **compared** by the host **computer** to determine whether they are the same. If they are not, the user is asked to repeat the procedure until they **match**. When they do **match**, the **password** is accepted and that particular user identity becomes locked until subsequently unlocked. As soon as the lock sequence is consummated in this manner, the following Terminal Locked Page is transmitted to the terminal for video **display**:

US PAT NO: 5,282,247 [IMAGE AVAILABLE] L17: 25 of 32
TITLE: Apparatus and method for providing data security in a computer system having removable memory

ABSTRACT:
A **computer** system having a memory card for storing data that is capable of being removed and reinserted and also having the. . . A passward is stored on the memory card. The memory card is set in a secure mode to prevent unauthorized **access** to the data stored on the memory card. Once the memory **card** is set in **secure** mode, it remains in secure mode, even when removed from the **computer** system and subsequently inserted back into that or another **computer** system. **Access** to the data is **permitted** when the memory **card** is set in **secure** mode only if a valid password is provided to the memory card.

DETDESC:

DETD(10)

If . . . elect to "lock" the memory card. Hence, the present invention involves a cooperative scheme between memory card 301 and the **computer** system 302. In the currently preferred embodiment of the present invention, the user prompts the **computer** system to issue the following commands to the memory **card**: SET.sub.-- **SECURE** which gives an authorized user the ability to set the memory **card** in **secure** mode; DISABLE.sub.-- SECURE which gives an authorized user the ability to disable secure mode; LOCK which prohibits unauthorized **access** to the stored data; and UNLOCK which **allows** an authorized user the capability to gain **access** to the stored data. The user also provides the memory card with one or more passwords via the **computer** system. The memory card notifies the **computer** system and user of its current state and status by sending an IDENTIFY.sub.-- DRIVE command response. The functions and interactions. . .

DETDESC:

US PAT NO: 5,424,5[redacted] [IMAGE AVAILABLE] [redacted] 11 of 15
TITLE: Personal scanner/computer for displaying shopping lists and scanning barcodes to aid shoppers

CLAIMS:

CLMS(18)

18. . . . comprising a shopping cart to which said barcode scanning device is mounted, and wherein said comparison routine includes means for **comparing** the string of characters **identifying** a scanned product decoded by said barcode reading device to the currently displayed shopping list, and, if any word of the product **identification** string **matches** any word of an entry on said shopping list, for displaying on said **display**/user input **device** all the possible **matches** having the **matching** word therein in a list of items having that word therein downloaded from another **computer** coupled to said processor by said modem/local area network interface device and for receiving a user selection of an item from said list entered via said **display**/user input **device**, and for extracting the price of said selected item from said price list and adding said price to a running total price for all items which have been scanned and for displaying the result on said **display**/user input **device**.

US PAT NO: 5,309,504 [IMAGE AVAILABLE] L4: 16 of 25
TITLE: Automated identification of attendant positions in a telecommunication system

DETDESC:

DETD(21)

Alternatively, the **terminal** identification numbers can be permanently stored in sequential order in memory locations 114, and the attendant identification numbers later written into the appropriate memory locations 112 in association with the **terminal ID** numbers. However, those skilled in the programming art can readily recognize that data can be stored in many different forms. . . changes positions, similar identification number entries are then programmed into the various memory locations so that specific attendants and data **terminals** 22 can be later associated. Essentially, the association between attendant identification numbers and the **terminal** identification numbers allows the **host** computer 18 to provide a **match** between a selected attendant at a position so that data can be sent to the **terminal**, also associated with that position.

US PAT NO: 4,893,248 [IMAGE AVAILABLE] L4: 19 of 25
TITLE: Monitoring and reporting system for remote terminals

DETDESC:

DETD(41)

Initialization in terms of entering initialization data into the RAM 38 of the remote **terminal** 10 is necessary before normal operation can commence. A first initialization is needed when the remote **terminal** 10 is first purchased or leased; typically, the program source has sold or leased the remote **terminal** 10 to the viewer and has entered the I.D. number of the remote **terminal** into an initializing computer, distinct from the above discussed **host** computer. Typically, the modem of the initializing computer has its own separate telephone number, typically an 800 number which may be called from anywhere in the United States or North America. Assuming that the remote **terminal** 10 has not been previously initialized and that the initialization data locations of the RAM 38 of the remote **terminal** 10 are void of this data, the initialization routine 300 is entered in the following fashion. In the first step 302, the power is applied to the remote **terminal** 10, whereby the serial interface 36 and the parallel input/output interface 26 are enabled. If the remote **terminal** 10 senses that the initialization data is absent from its RAM 38, it accesses in step 304 a known location in its ROM 34, containing the telephone number of the initialization computer. Next, in step 306, the remote **terminal** places a telephone call to the initialization computer and in step 308 transmits a message with the unique **ID** of the remote **terminal** 10 to the initialization computer. In response, the back-up computer compares the **ID** number with those retained in its memory. If a **match** is made indicating that the transmitted **ID** is valid, the initialization computer downloads in step 310 the initialization data as identified above. Next, step 312 inputs the. . .

US PAT NO: 5,465,084 [IMAGE AVAILABLE] L5: 14 of 31
TITLE: Method to provide security for a computer and a device therefor

DETDESC:

DETD(5)

FIG. 2 shows how a computer display or **terminal** might display a 10.times.10 array. Such a matrix or other geometric configuration will be presented by the computer on the display used by someone attempting to gain **access** to the computer or associated network. Such a matrix or other geometric arrangement of elements will be presented on the display used by someone attempting to gain **access** to the computer or network. The **password** of the user is entered into the array by any of various methods; the usual method being to first select. . . When the pattern is complete, the user sends a signal to the computer which then proceeds to search for a **matching** pattern in memory. Because the pattern is not read until all of the elements have been entered, the order of. . .

US PAT NO: 5,857,024 [IMAGE AVAILABLE] L5: 2 of 31
TITLE: IC card and authentication method for information processing apparatus

SUMMARY:

BSUM(6)

With . . . shown in FIG. 6A, security is maintained by permitting an information processing apparatus to perform a process only when a **match** is obtained between a **password** input and a **password** previously registered. For example, when network **access** is sought by a **terminal** device on a network, the network issues a request to the **terminal** device for the input of a **password**, and grants **access** permission only when the **password** input **matches** one that was previously registered. A cash dispenser (automatic teller machine) is another well known information processing example. To make. . . cash dispenser, a cash card must be inserted into the cash dispenser, and an identification number, which corresponds to a **password** and which was previously registered, must then be input.